(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2005 年1 月20 日 (20.01.2005)

PCT

(10) 国際公開番号
WO 2005/006204 A1

(51) 国際特許分類[7]: G06F 15/00, 12/00, 12/14

(21) 国際出願番号: PCT/JP2004/009847

(22) 国際出願日: 2004 年7 月9 日 (09.07.2004)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2003-273602 2003 年7 月11 日 (11.07.2003) JP

(71) 出願人 (米国を除く全ての指定国について): 日本電信電話株式会社 (NIPPON TELEGRAPH AND TELEPHONE CORPORATION) [JP/JP]; 〒1008116 東京都千代田区大手町二丁目3番1号 Tokyo (JP).

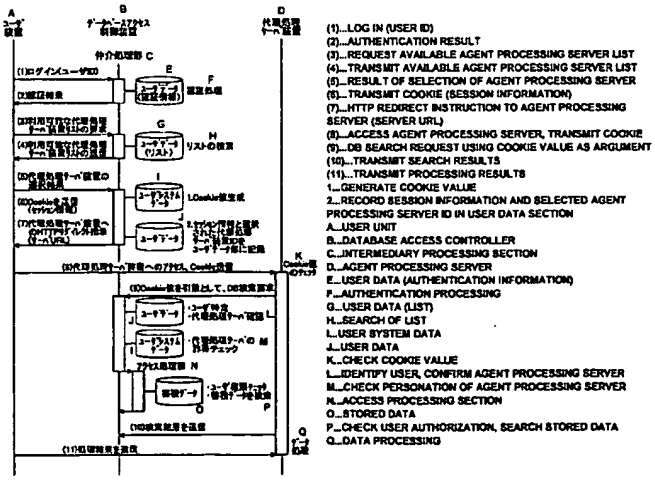
(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 今枝 尚史 (IMAEDA, Takashi) [JP/JP]; 〒1808585 東京都武蔵野市緑町3丁目9-11 NTT知的財産センタ内 Tokyo (JP). 遠藤 公誉 (ENDO, Kimitaka) [JP/JP]; 〒1808585 東京都武蔵野市緑町3丁目9-11 NTT知的財産センタ内 Tokyo (JP). 中山 丈二 (NAKAYAMA, Jouji) [JP/JP]; 〒1808585 東京都武蔵野市緑町3丁目9-11 NTT知的財産センタ内 Tokyo (JP). 山本 哲也 (YAMAMOTO, Tetsuya) [JP/JP]; 〒1808585 東京都武蔵野市緑町3丁目9-11 NTT知的財産センタ内 Tokyo (JP). 下倉 健一朗 (SHIMOKURA, Ken-ichiro) [JP/JP]; 〒1808585 東京都武蔵野市緑町3丁目9-11 NTT知的財産センタ内 Tokyo (JP). 藪内 勉 (YABUUCHI, Tsutomu) [JP/JP]; 〒1808585 東京都武蔵野市緑町3丁目9-11 NTT知的財

[続葉有]

(54) Title: DATABASE ACCESS CONTROL METHOD, DATABASE ACCESS CONTROLLER, AGENT PROCESSING SERVER, DATABASE ACCESS CONTROL PROGRAM, AND MEDIUM RECORDING THE PROGRAM

(54) 発明の名称: データベースアクセス制御方法、データベースアクセス制御装置、代理処理サーバ装置、データベースアクセス制御のためのプログラム、および該プログラムを記録した記録媒体



(57) Abstract: According to the user ID of a user unit, a database access controller generates an access key and stores it. The database access controller transmits the access key to the user unit along with the address of an agent processing server. The user unit transmits the access key when it requests database access made by the agent processing server, which transmits the access key when it requests database processing performed by the database access controller. Upon receiving the database processing request, the database access controller checks whether the database access controller stores the same access key as that received from the agent processing server and accesses the database only when the access key is stored.

(57) 要約: データベースアクセス制御装置は、ユーザ装置のユーザＩＤに基づき、アクセス鍵を生成して格納しておく。そして、データベースアクセス制御装置は、該アクセス鍵を、代理処理サーバ装置のアドレスとともにユーザ装置に送信する。ユーザ装置は、代理処理サーバ装置にデータベースアクセス要求を行う際にアクセス鍵を送信

[続葉有]

WO 2005/006204 A1

産センタ内 Tokyo (JP). 手塚 博久 (TEZUKA, Hirohisa) [JP/JP]; 〒1808585 東京都武蔵野市緑町３丁目９−１１ＮＴＴ知的財産センタ内 Tokyo (JP). 浦野 将人 (URANO, Masato) [JP/JP]; 〒1808585 東京都武蔵野市緑町３丁目９−１１ＮＴＴ知的財産センタ内 Tokyo (JP).

(74) 代理人: 伊東 忠彦 (ITOH, Tadahiko); 〒1506032 東京都渋谷区恵比寿４丁目２０番３号 恵比寿ガーデンプレイスタワー３２階 Tokyo (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

し、代理処理サーバ装置は、データベースアクセス制御装置にデータベース処理要求を行う際にアクセス鍵を送信する。データベースアクセス制御装置は、データベース処理要求を受信した際に、該代理処理サーバ装から受信したアクセス鍵と同じアクセス鍵を、データベースアクセス制御装置が格納しているか否かを判定し、該アクセス鍵を有している場合に限り、データベースにアクセスする。

明 細 書

データベースアクセス制御方法、データベースアクセス制御装置、代理処理サーバ装置、データベースアクセス制御のためのプログラム、および該プログラムを記録した記録媒体

技術分野

[0001] 本発明は、データベースのアクセス制御技術に関し、詳しくは、データベースアクセス制御装置とユーザの代理としての代理処理サーバ装置との連携によりデータベースへのアクセスを行うデータベースアクセス制御技術に関する。

背景技術

[0002] 一般にデータベースは、複数のユーザがデータを保存しているため、どのユーザがどのデータを登録、参照、更新、または削除できるかはデータベースのアクセス制御機構によって制御されている。以下、データベースへのデータの登録、参照、更新、削除をまとめてデータベースへのアクセスと呼ぶことにする。例えば、データベースのアクセス制御機構では、ユーザAのデータにはユーザBはアクセスできず、またユーザBのデータにはユーザAはアクセスできないようにアクセス制御が行われる。

[0003] このデータベースのアクセス制御方法としては、従来から、ユーザがデータベースに対して渡すユーザIDとパスワードの組等の認証情報を、データベースのアクセス制御機構にあらかじめ登録してある認証情報と比較することによりアクセスしようとしているユーザを特定し、次に特定されたユーザに対してどのデータにアクセスして良いかが設定されているアクセス制御リスト(Access Control List)に基づいて各データのアクセスに対しての許可、不許可を決定するという方式がある。

[0004] これは既存の多くのデータベースに用いられている方法であり、データベースをアクセスするための言語の規格であるSQL92ではgrant文、revoke文によってアクセス制御リストにアクセス権限の情報を追加、削除することにより、ユーザに対するデータへのアクセス権限の付与、取り消しを行うよう規定されている。

[0005] 上記のアクセス制御方式はデータベースへのアクセスがデータベースにデータを格納しているユーザのみの場合のものである。一方、それとは異なる形態として、デ

ータベースへのアクセスをデータを格納しているユーザではなく、ユーザの代わりにデータベースへのアクセスを行う代理エージェント(代理処理サーバ)が行う方法がある。これはユーザが代理エージェントにデータベースへのアクセスを依頼するという方法で行われる。これは、例えばデータを加工処理する機能を代理エージェントが提供しており、ユーザはデータベースに保存してあるデータを代理エージェントに加工処理してもらい、ユーザはその処理結果を受け取るような場合である。

[0006] ユーザの代理として代理エージェントがデータベースへアクセスを行う場合に考慮すべきことは、代理エージェントが依頼主のユーザのアクセス権限に基づいてデータベースへのアクセスを行うようにしなければならないという点である。例えば、あるユーザAが代理エージェントに対してデータベースへのアクセスを依頼するときに、代理エージェントはユーザAに対してアクセスが許可されているデータしかアクセスできないようにアクセス制御されなければならない。すなわちユーザAの依頼にもかかわらず、代理エージェントがユーザAに許可されていないユーザBのデータにアクセスし、その情報をユーザAに返すようなことはあってはならない。代理エージェントが依頼主のユーザのアクセス権限に基づいてデータベースにアクセスすることをユーザから代理エージェントへのアクセス権限の委譲と呼ぶ。

[0007] 上記のような条件を満たすアクセス制御方法のもっとも単純なものとしては、ユーザが代理エージェントに対しデータベースにアクセスするための自分のユーザIDやパスワード等の認証情報を渡し、代理エージェントがその認証情報を利用してデータベースにアクセスしてそのユーザのデータを取得するという方法がある。

[0008] また、別の方法としては、デジタル署名技術や暗号通信技術を利用して、ユーザによる代理エージェントへのアクセス権限の委譲が正しいものかどうかをデジタル証明書やデジタル署名、暗号化や一方向関数を用いて確認するものがある(例えば、文献1:特開2001−101054号公報、文献2:特開2002−163235号公報参照)。

[0009] しかし、ユーザが代理エージェントへ自分の認証情報を渡し、代理エージェントがその認証情報を利用してデータベースへアクセスする方法には次の問題がある。一般に代理エージェントはユーザとは異なる第三者の実体であり、ユーザは代理エージェントを必ずしも信頼することができない。そのため、例えば、ユーザAが代理エー

ジェントにユーザIDとパスワード等の認証情報を渡してしまうと、代理エージェントはその認証情報を内部に保持しておき、他ユーザであるユーザBがアクセスしたときにその保持しておいた認証情報を使ってユーザAになりすまし、ユーザBには許可されていないはずのユーザAのデータにアクセスを許してしまうというような悪意を持った処理を代理エージェントが行う可能性がある。

[0010] また、デジタル署名技術や暗号通信技術を利用してアクセス権限の委譲等を確認する方法では、デジタル証明書やデジタル署名、暗号化、一方向関数など複雑な処理を行わなければならず、またユーザ、代理エージェント、データベース間で鍵情報や認証情報などのやりとりを何ステップも行わなければならない。またこれらの方法はアクセス権限を委譲するための方式に関してのみに用いられる方法であり、この方法を用いても、委譲されたアクセス権限に基づいてデータベースにアクセスした結果が委譲もとのユーザに確実に返されることは保証されていない。従って、この方法は、ユーザがデータベースのアクセスを依頼する代理エージェントへの適用には適切でない。

発明の開示

発明が解決しようとする課題

[0011] 本発明は、上記のような課題を解決するためになされたものであり、代理エージェント(代理処理サーバ)がデータベースまたはデータベース相当の機能における許可されていないアクセスをすることを防止する仕組みを提供することを目的とする。

課題を解決するための手段

[0012] 本発明では、データベースアクセス制御装置は、ユーザ装置からの要求に応じて、利用可能な代理処理サーバ装置のアドレスを該ユーザ装置に送信する。ユーザ装置は、上記アドレスの代理処理サーバ装置に接続してデータベースアクセス要求を行い、代理処理サーバ装置は、ユーザ装置からのデータベースアクセス要求に従いデータベースアクセス制御装置にデータベース処理要求を行う。データベースアクセス制御装置は、代理処理サーバ装置からのデータベース処理要求に応じてデータベースへの処理を実行し、該処理結果を前記代理処理サーバ装置に送信する。代理処理サーバ装置は、前記データベースアクセス制御装置から送信された処理結果

に対して依頼された処理を実行し、該処理結果を前記ユーザ装置に送信する。

[0013] さらに、本発明では、データベースアクセス制御装置は、ユーザ装置のユーザIDに基づきアクセス鍵を生成し、該アクセス鍵を前記データベースアクセス制御装置の記憶手段に格納するとともに、前記ユーザ装置に送信する。ユーザ装置は、代理処理サーバ装置にデータベースアクセス要求を行う際にアクセス鍵を代理処理サーバ装置に送信し、代理処理サーバ装置は、データベースアクセス制御装置にデータベース処理要求を行う際にアクセス鍵を前記データベースアクセス制御装置に送信する。データベースアクセス制御装置では、代理処理サーバ装置から受信したアクセス鍵と同じアクセス鍵が前記記憶手段に存在するか否かを調べ判定し、該アクセス鍵が存在する場合に限り、アクセス鍵に対応するユーザIDに対して許可された限度内で、データベース中のデータへのアクセスを実行するようにする。

[0014] また、本発明では、データベースアクセス制御装置は、アクセス鍵の判定に加えて、ユーザ装置が当該代理処理サーバ装置に接続中の状態にあるかを判定し、前記ユーザ装置が当該代理処理サーバ装置に接続中の状態にある場合に限り、データベース中のデータへのアクセスを実行するようにする。

[0015] なお、上記の構成において、データベース処理要求とは、データベースに対するデータ登録、変更、削除、もしくは検索等の処理の要求のことである。

発明の効果

[0016] 本発明によれば、代理処理許可を与えられていない代理処理サーバ装置はデータベースアクセス処理を実行できず、また代理処理許可を与えられた代理処理サーバ装置でも代理処理を依頼したユーザIDの権限を越えるデータベースに対するデータ登録、変更、削除、もしくは検索等の処理を実行することができない。

[0017] また、ユーザ装置からの検索代行処理依頼を受けることなく、代理処理サーバ装置が独自にデータベース検索処理を実行することも禁止されている。このため、代理処理サーバ装置の利用者は不正な行為が行われることを心配することなく、データベース検索を実施する処理および、その検索結果を加工処理する代理処理サーバ装置を利用することが可能となる。それにより、ユーザは第三者が用意する様々な有用な処理を行う代理処理サーバ装置を利用することが可能になる。

図面の簡単な説明

[0018] [図1]本発明が適用されるシステム全体の構成図である。

[図2]データベース保存データの一例を示す図である。

[図3]本発明の一実施例の処理シーケンス図である。

[図4]本発明の一実施例の各装置間の連携図である。

符号の説明

[0019] 100 データベースアクセス制御装置

101 仲介処理部

102 アクセス処理部

200 データベース

210 ユーザデータ部

220 ユーザシステムデータ部

230 蓄積データ部

300 代理処理サーバ装置

400 ユーザ装置

500 ネットワーク

発明を実施するための最良の形態

[0020] 以下、本発明の実施の形態を図面により詳しく説明する。

実施例 1

[0021] 図1に本発明が適用されるシステム全体の構成図を示す。図1において、100はデータベースアクセス制御装置、200は複数のユーザで共用されるデータベース、300は代理処理サーバ装置、400は各ユーザのユーザ装置、500はインターネット等のネットワークである。データベースアクセス制御装置100は、ユーザ装置400と代理処理サーバ装置300との仲介機能を有する仲介処理部101、およびデータベース200の蓄積データへのアクセス機能を有するアクセス処理部102から構成される。

[0022] データベース200は、あらかじめ登録されたユーザIDや認証情報等のユーザに関する情報、代理処理サーバ装置300の情報、および本システムが提供するための蓄

積データを保持する。さらに、図1では省略しているが、データベース200はアクセス制御機構を内蔵している。このデータベースアクセス制御装置100とデータベース200との接続は直接あるいはネットワークを介してのいずれでもよい。

[0023] 以下、代理処理サーバ装置を経由して、データベース装置から、データの検索結果を取得する場合を例のとり説明する。なお、以下説明するようなデータ検索以外にも、データ登録、更新、削除、検索等の様々な処理に本発明を適用することが可能である。

[0024] データベースアクセス制御装置100、代理処理サーバ装置300、およびユーザ装置400は、ネットワーク500を介して接続されている。データベースアクセス制御装置100および代理処理サーバ装置300の実体はコンピュータであり、CPUやメモリ等のハードウェア資源の環境下で、プログラムによって各処理を実行する。ここでは、ユーザの代理として、データベースアクセス制御装置100と代理処理サーバ装置300とが連携して動作することにより、データベース200へのアクセスを実行し、読み出した蓄積データに所望の処理を施し、その結果を該当ユーザのユーザ装置400に対して送信する。

[0025] 図2はデータベース200における保存データの一例である。データベース200はユーザデータ部210、ユーザシステムデータ部220、蓄積データ部230から構成される。ユーザデータ部210は登録されたユーザに関する情報を保存するもので、ユーザ毎に、ユーザID211、認証情報212、ユーザ権限情報213、セッション情報214、代理サーバリスト215、接続中の代理処理サーバID216を保存する。ユーザシステムデータ部220はユーザを代理するシステム情報を保持するもので、ここでは代理処理サーバ装置300のID(代理処理サーバID)221、そのURL(代理処理サーバURL)222を保持する。蓄積データ部230はデータ231及びその閲覧可能権限情報232を保持する。

[0026] 図3に本実施例の全体処理シーケンス例を示す。また、図4に各装置間の連携図を示す。図3及び図4を参照して、以下では、ユーザ装置400、データベースアクセス制御装置100、および代理処理サーバ装置300の3者間を接続するプロトコルとしてHTTPを利用した例を説明する。

[0027] まず、ユーザはユーザ装置400から、事前にデータベース200のユーザデータ部210に保存されたユーザID211を用いてデータベースアクセス制御装置100にログインする(ステップ1)。このとき、データベースアクセス制御装置100の仲介処理部101は、同じくデータベース200のユーザデータ部210に保存された各ユーザID211毎の認証情報212を用いて認証処理を行う。これにより、データベースアクセス制御装置100の仲介処理部101は、ログインしようとするユーザが事前に登録された正規のユーザであることを確認し、認証結果をユーザ装置400に送信する(ステップ2)。

[0028] 次に、ユーザ装置400は、データベースアクセス制御装置100に対して、当該ユーザが利用可能な代理処理サーバ装置300のリストを要求するコマンドを送信し(ステップ3)、これを受信したデータベースアクセス制御装置100の仲介処理部101は、データベース200のユーザデータ部210から当該ユーザが利用可能な代理処理サーバ装置300のリスト215を読み出し、ユーザ装置400に送信する(ステップ4)。ユーザ装置400は、受信した代理処理サーバリストを画面表示する。ユーザによって、この表示された利用可能な代理処理サーバの中から利用しようとする代理処理サーバ装置300が選択されると、ユーザ装置400は、その結果をデータベースアクセス制御装置100に送信する(ステップ5)。ユーザ装置400は、ステップ5において、ユーザからの入力に基づき、代理処理サーバ300における処理(データベースアクセス等)に必要な情報も送信する。

[0029] データベースアクセス制御装置100の仲介処理部101は、ユーザ装置400から選択された代理処理サーバ装置300の情報を受信すると、データベース200のユーザデータ210内の、当該ユーザの利用可能な代理処理サーバ装置300のリスト215を検索し、選択された代理処理サーバ装置300の利用が当該ユーザに許可されていることを確認する。その後、仲介処理部101は、当該ユーザIDに基づいて乱数(セッション情報)を生成し、この生成されたセッション情報からCookie(アクセス鍵)を生成し、これを当該ユーザのユーザ装置400に送信するとともに(ステップ6)、データベース200のユーザシステムデータ部220から、選択された代理処理サーバ装置300のURL222を取得し、URL222をユーザ装置400に送信することにより、HTTPリダイレクト応答によって前記ユーザ装置400に対し当該代理処理サーバ装置300にリ

ダイレクト接続することを指示する(ステップ7)。また、仲介処理部101は、データベース200のユーザデータ部210に、前記生成したセッション情報214と前記接続しようとする代理処理サーバ装置300のID番号216を記録する。

[0030] ユーザ装置400は、代理処理サーバ装置300にリダイレクト接続するにあたって、データベースアクセス制御装置100から受信したCookieの値を代理処理サーバ装置300に送信する(ステップ8)。

[0031] 代理処理サーバ装置300は、ユーザ装置400からのHTTPリクエストである接続要求コマンドの中に含まれたCookieの値を取り出す。そして、代理処理サーバ装置300は、そのCookieの値と、ユーザから指定された処理に必要な蓄積データのテーブルを指定する値と、及び検索に用いる値とを、HTTPリクエストの引数として、データベースアクセス制御装置100にHTTPリクエスト(データベース検索要求)を送信する(ステップ9)。また、データベース検索要求とともに代理処理サーバ装置300のIDがデータベースアクセス制御装置100に送信される。

[0032] 代理処理サーバ装置300からのHTTPリクエスト(データベース検索要求)を受信したデータベースアクセス制御装置100の仲介処理部101は、まず、リクエストの中に設定された引数を取り出す。そして、引数の中のCookieの値からセッション情報を取り出し、そのセッション情報と、データベース200のユーザデータ部210のセッション情報214とを比較して、代理処理サーバ装置300に対してHTTPリクエストを発したユーザ装置400のユーザIDを特定する(ユーザ特定)。ユーザIDが存在している場合は、代理処理サーバ装置300から受信した代理処理サーバ装置300のID番号を取得し、データベース200のユーザデータ部210の該当のユーザIDに対応する接続中の代理処理サーバ装置300のID番号216と、上記のID番号とを比較し、一致するかどうかを確認する(代理処理サーバ確認)。一致する場合、代理処理サーバ装置300のIDがユーザシステムデータ部220に存在するかどうかを確認する(代理処理サーバの詐称チェック)。更に、当該ユーザIDのユーザに代理処理サーバ装置300の利用許可があるか否かを、代理処理サーバリスト215により確認する処理を行ってもよい。

[0033] セッション情報に対応するユーザIDが存在しない場合、もしくは、受信した代理処

理サーバ装置300のID番号と、接続中の代理処理サーバIDとして記録されていたID番号とが一致しない場合、もしくは、代理処理サーバ装置300のIDがユーザシステムデータ部220に存在しない場合、データベースアクセス制御装置100の仲介処理部101は、代理処理サーバ装置300に対しエラー応答し、以降の処理は実行しない。

[0034] ユーザIDが存在し、かつ、代理処理サーバ装置300のID番号が一致し、かつ、代理処理サーバ装置300のIDがユーザシステムデータ部220に存在した場合は、仲介処理部101は、データベース200の蓄積データ部230にアクセスするため、HTTPリクエスト中に含まれる残りの引数情報をアクセス処理部102に渡す。

[0035] データベースアクセス制御装置100のアクセス処理部102は、仲介処理部101から渡された引数に従って、データベース200の蓄積データ230の検索を実行する。このとき、蓄積データ230にユーザIDごとの閲覧権限情報232が設定されている場合は、データベース200のユーザデータ部210において該当のユーザIDに設定されているユーザ権限情報213と蓄積データ230の閲覧可能権限情報232とが合致している場合のみ検索を実行できる(ユーザ権限チェック)。アクセス処理部102によって検索された結果は仲介処理部101に渡され、仲介処理部101は、その結果を代理処理サーバ装置300からのHTTPリクエストに対するHTTP応答の形で代理処理サーバ装置300に送信する(ステップ10)。

[0036] なお、代理処理サーバ装置300とデータベースアクセス制御装置100との間のHTTPリクエストおよび応答は、代理処理サーバ装置300の処理に必要とされる蓄積データ検索の分だけ複数回実行することも可能である。

[0037] 代理処理サーバ装置300は、データベースアクセス制御装置100の仲介処理部101から受信したHTTP応答の中に含まれる蓄積データに対して、必要なデータ処理(データマイニングを行う処理や、代理処理サーバ装置300自体が有するデータベースに保存された関連するデータと組み合わせた処理等)を実行し、その結果をユーザ装置400にHTTP応答の形で送信する(ステップ11)。

[0038] 上記動作において、ユーザ装置400がデータベースアクセス制御装置100から受信した代理処理サーバ装置300のリストの中から1つが選択され、選択結果がデータ

ベースアクセス制御装置100に送信される。そして、データベースアクセス制御装置100の仲介処理部101は、データベース200のユーザデータ部210に上記選択された代理処理サーバ装置300のID番号を接続中の代理処理サーバ装置300のID番号216として記録する。この後、ユーザ装置400が別の代理処理サーバ装置300に接続するために、再度、代理処理サーバ装置300のリスト表示を実行したり、データベースアクセス制御装置100で提供される別のサービスのための操作を行うと、先のデータベース200のユーザデータ部210に保存された代理処理サーバ装置300のID番号(216)は消去あるいは書き換えられる。また、セッション情報もユーザIDのログインの度に異なる値が生成される。

[0039] このため、代理処理サーバ装置300が一度接続されたユーザ装置400からのCookieの値を保存しておき、ユーザ装置400からの要求を受けずに独自にデータベースアクセス制御装置100への接続を行おうとしても、Cookieの値に含まれるセッション情報を元に、データベースアクセス制御装置100の仲介処理部101はユーザを特定できないため、その代理処理サーバ装置300から要求された検索処理を実行しない。更に、代理処理サーバ装置300がユーザ装置400からの要求を受けずに独自にデータベースアクセス制御装置100への接続を行う場合には、データベース200のユーザデータ部210に当該代理処理サーバ装置300のID番号が接続中の代理処理サーバ装置300のID番号216として記録されていないことからも、データベースアクセス制御装置100の仲介処理部101は、その代理処理サーバ装置300から要求された検索処理を実行しない。

[0040] また、ユーザ装置400がデータベースアクセス制御装置100から受信したリストに表示される代理処理サーバ装置300以外のURLを直接指定し、別の代理処理サーバ装置用に作成されたCookieを用いて接続を行おうとしても、その代理処理サーバのIDは、データベースアクセス制御装置100のユーザデータ部に、接続中の代理処理サーバ216として記録されていないので、データベースアクセス制御装置100の仲介処理部101は、その代理処理サーバ装置300から要求された検索処理を実行しない。これにより、ユーザ装置400がリスト表示された代理処理サーバ装置300以外の代理処理サーバ装置を利用することを禁止できる。

[0041] なお、図1で示したデータベースアクセス制御装置100における一部もしくは全部の処理機能をコンピュータのプログラムで構成し、そのプログラムをコンピュータを用いて実行して本発明を実現することができる。あるいは、図2で示した処理シーケンス手順をコンピュータのプログラムで構成し、そのプログラムをコンピュータに実行させることができる。また、コンピュータでその処理機能を実現するためのプログラム、あるいは、コンピュータにその処理手順を実行させるためのプログラムを、そのコンピュータが読み取り可能な記録媒体、例えば、FDや、MO、ROM、メモリカード、CD、DVD、リムーバブルディスクなどに記録して、保存したり、提供したりすることができるとともに、インターネット等のネットワークを通してそのプログラムを配布したりすることが可能である。

[0042] 本発明は、上記の各実施の形態に限定されることなく、特許請求の範囲内で種々変更・応用が可能である。

請求の範囲

[1] ユーザ装置からの要求に応じて、データベースアクセス制御装置と代理処理サーバ装置とが連携してデータベースへのアクセス制御を行う方法であって、

前記データベースアクセス制御装置は、ユーザ装置からの要求に応じて、利用可能な代理処理サーバ装置のアドレスを該ユーザ装置に送信し、

前記ユーザ装置は、前記アドレスの代理処理サーバ装置に接続してデータベースアクセス要求を行い、

前記代理処理サーバ装置は、前記ユーザ装置からのデータベースアクセス要求に従い前記データベースアクセス制御装置にデータベース処理要求を行い、

前記データベースアクセス制御装置は、前記代理処理サーバ装置からのデータベース処理要求に応じてデータベースへの処理を行い、該処理結果を前記代理処理サーバ装置に送信し、

前記代理処理サーバ装置は、前記データベースアクセス制御装置から送信された処理結果に対して付加処理を実行し、該付加処理結果を前記ユーザ装置に送信する、ことを特徴とするデータベースアクセス制御方法。

[2] 前記データベースアクセス制御装置は、前記ユーザ装置のユーザIDに基づきアクセス鍵を生成し、該アクセス鍵を前記データベースアクセス制御装置の記憶手段に格納するとともに、前記ユーザ装置に送信し、

前記ユーザ装置は、前記代理処理サーバ装置にデータベースアクセス要求を行う際に前記アクセス鍵を前記代理処理サーバ装置に送信し、

前記代理処理サーバ装置は、前記データベースアクセス制御装置にデータベース処理要求を行う際に前記アクセス鍵を前記データベースアクセス制御装置に送信し、

前記データベースアクセス制御装置は、前記代理処理サーバ装置から受信したアクセス鍵と同じアクセス鍵が前記記憶手段に存在するか否かを調べ、該アクセス鍵が存在する場合に限り、前記アクセス鍵に対応するユーザIDに対して許可された限度内で、データベース中のデータへのアクセスを実行する、ことを特徴とする請求項1に記載のデータベースアクセス制御方法。

[3] 前記データベースアクセス制御装置は、前記アクセス鍵の判定に加えて、前記ユーザ装置が当該代理処理サーバ装置に接続中の状態にあるかを判定し、前記ユーザ装置が当該代理処理サーバ装置に接続中の状態にある場合に限り、前記データベース中のデータへのアクセスを実行する、ことを特徴とする請求項2に記載のデータベースアクセス制御方法。

[4] ユーザ装置からの要求に応じて、代理処理サーバ装置と連携してデータベースへのアクセス制御を行うデータベースアクセス制御装置であって、

前記ユーザ装置からの要求に応じて、利用可能な代理処理サーバ装置のアドレスを該ユーザ装置に送信することにより、前記ユーザ装置に前記代理処理サーバ装置への接続を指示する手段と、

前記代理処理サーバ装置からのデータベース処理要求に応じてデータベースへの処理を実行し、処理結果を前記代理処理サーバ装置に送信する手段と、を有することを特徴とするデータベースアクセス制御装置。

[5] 前記ユーザ装置のユーザIDに基づきアクセス鍵を生成し、該アクセス鍵を前記データベースアクセス制御装置の記憶手段に格納するとともに、該アクセス鍵を、前記代理処理サーバ装置のアドレスを前記ユーザ装置に送信する際に併せて前記ユーザ装置に送信する手段と、

前記代理処理サーバ装置からアクセス鍵とデータベース処理要求を受信し、前記代理処理サーバ装置から受信したアクセス鍵と同じアクセス鍵が前記記憶手段に存在するか否かを調べる手段と、

前記アクセス鍵が存在する場合に限り、前記アクセス鍵に対応するユーザIDに対して許可された限度内で、データベース中のデータへのアクセスを実行する手段、を更に有することを特徴とする請求項4に記載のデータベースアクセス制御装置。

[6] 前記データベースアクセス制御装置は、前記アクセス鍵の判定に加えて、前記ユーザ装置が当該代理処理サーバ装置に接続中の状態にあるかを判定し、前記ユーザ装置が当該代理処理サーバ装置に接続中の状態にある場合に限り、前記データベース中のデータへのアクセスを実行する、ことを特徴とする請求項5に記載のデータベースアクセス制御装置。

[7] ユーザ装置からの要求に応じ、データベースアクセス制御装置を介してデータベースへのアクセスを行う代理処理サーバ装置であって、

前記ユーザ装置から、アクセス鍵とデータベースアクセス要求を受信する手段と、

前記データベースアクセス制御装置に、データベース処理要求とともに前記アクセス鍵を送信する手段と、

前記データベース処理要求に応じたデータベースの処理結果を前記データベースアクセス制御装置から受信し、当該処理結果に対して付加処理を実行し、該付加処理結果を前記ユーザ装置に送信する手段と、を有することを特徴とする代理処理サーバ装置。

[8] ユーザ装置からの要求に応じて、代理処理サーバ装置と連携してデータベースへのアクセス制御を行うデータベースアクセス制御処理をコンピュータに実行させるプログラムであって、

前記ユーザ装置からの要求に応じて、利用可能な代理処理サーバ装置のアドレスを該ユーザ装置に送信することにより、前記ユーザ装置に前記代理処理サーバ装置への接続を指示する手順と、

前記代理処理サーバ装置からのデータベース処理要求に応じてデータベースへの処理を実行し、処理結果を前記代理処理サーバ装置に送信する手順と、をコンピュータに実行させるプログラム。

[9] 前記ユーザ装置のユーザIDに基づきアクセス鍵を生成し、該アクセス鍵を前記データベースアクセス制御装置の記憶手段に格納するとともに、該アクセス鍵を、前記代理処理サーバ装置のアドレスを前記ユーザ装置に送信する際に併せて前記ユーザ装置に送信する手順と、

前記代理処理サーバ装置からアクセス鍵とデータベース処理要求を受信し、前記代理処理サーバ装置から受信したアクセス鍵と同じアクセス鍵が前記記憶手段に存在するか否かを調べる手順と、

前記アクセス鍵が存在する場合に限り、前記アクセス鍵に対応するユーザIDに対して許可された限度内で、データベース中のデータへのアクセスを実行する手順、とをコンピュータに実行させる請求項8に記載のプログラム。

[10] 前記アクセス鍵の判定に加えて、前記ユーザ装置が当該代理処理サーバ装置に接続中の状態にあるかを判定し、前記ユーザ装置が当該代理処理サーバ装置に接続中の状態にある場合に限り、前記データベース中のデータへのアクセスを実行する手順をコンピュータに実行させる請求項9に記載のプログラム。

[11] 請求項8ないし10のうちいずれか1項に記載のプログラムを記録したコンピュータ読み取り可能な記録媒体。

[12] ユーザ装置からの要求に応じ、データベースアクセス制御装置を介してデータベースへのアクセスを行う代理処理をコンピュータに実行させるプログラムであって、

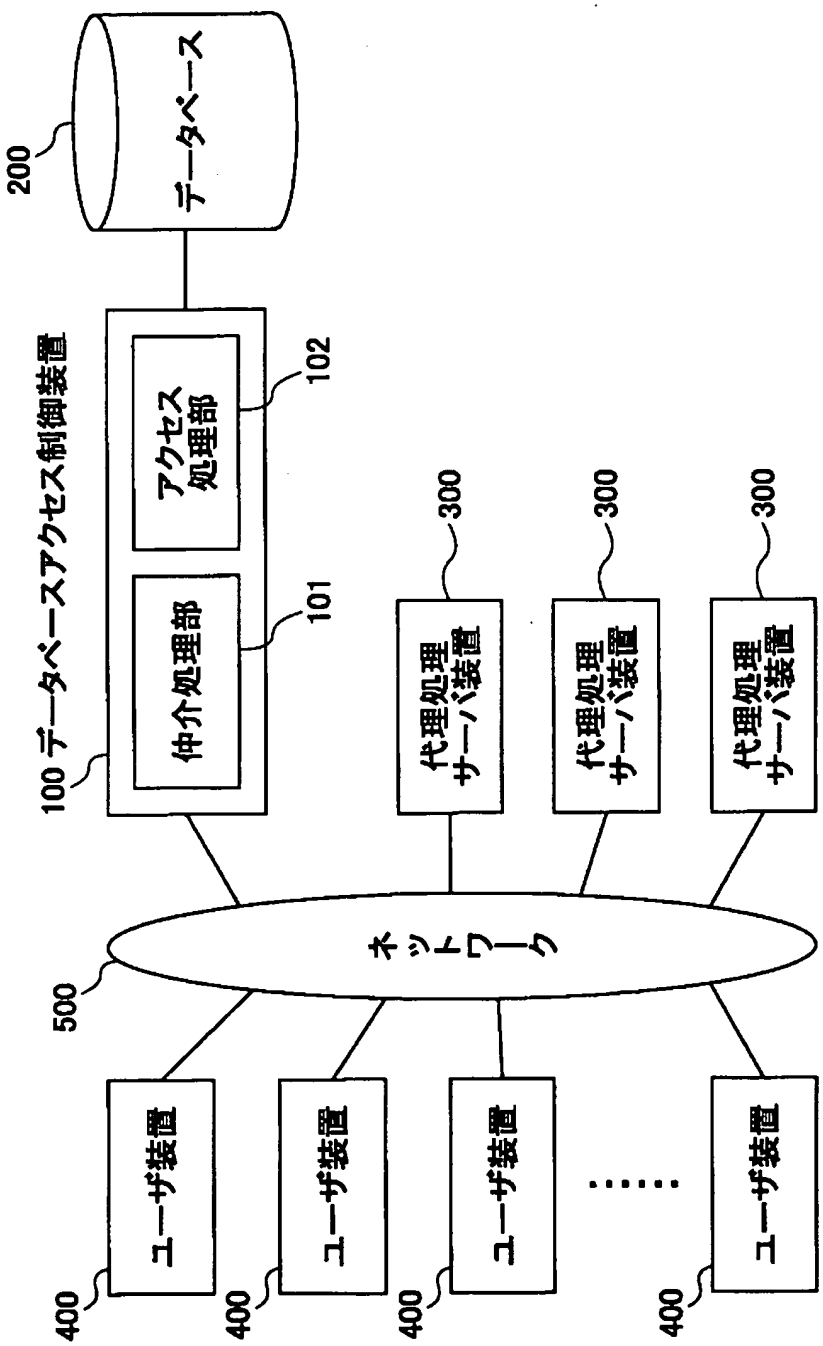
前記ユーザ装置から、アクセス鍵とデータベースアクセス要求を受信する手順と、

前記データベースアクセス制御装置に、データベース処理要求とともに前記アクセス鍵を送信する手順と、

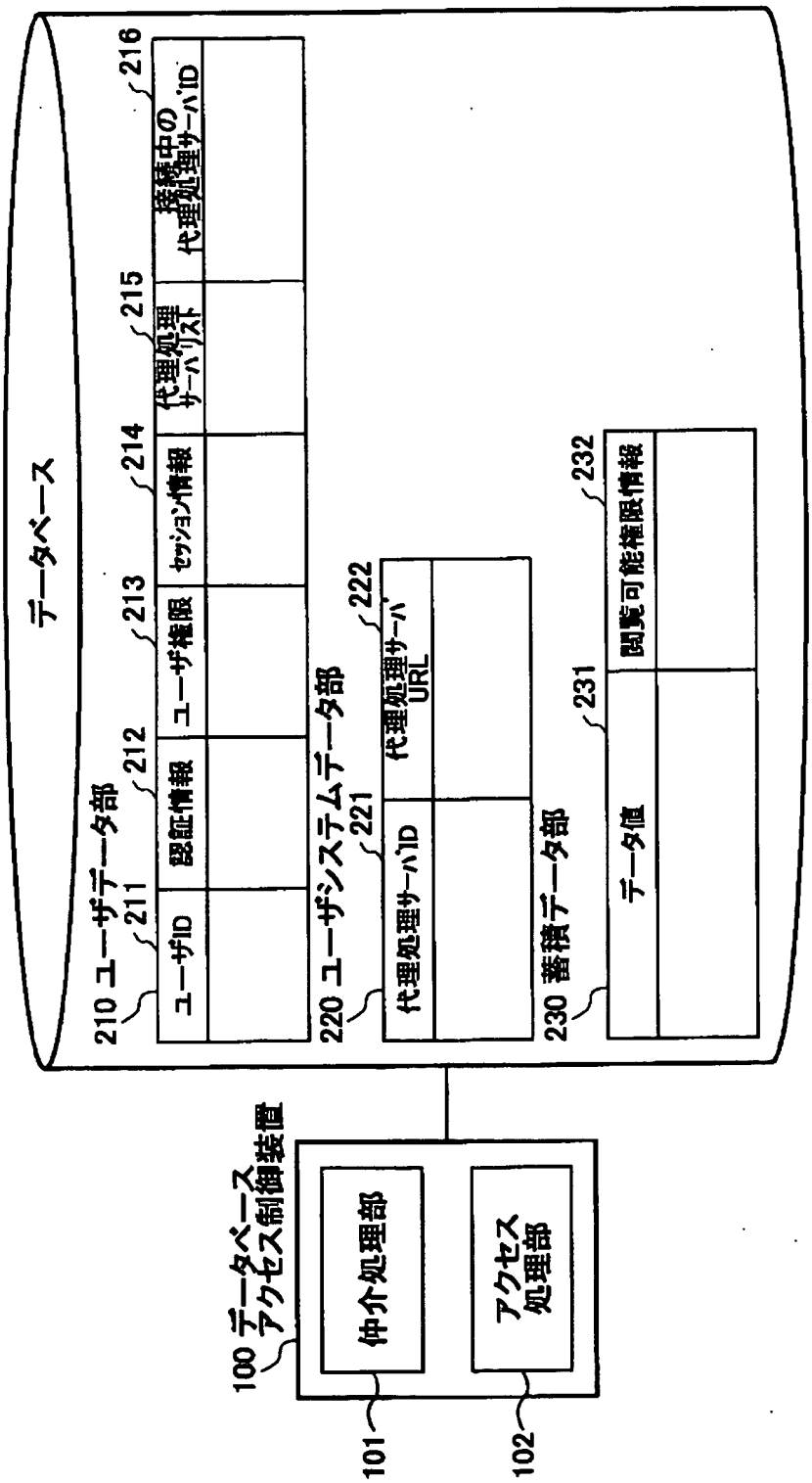
前記データベース処理要求に応じたデータベースの処理結果を前記データベースアクセス制御装置から受信し、当該処理結果に対して付加処理を実行し、該付加処理結果を前記ユーザ装置に送信する手順と、をコンピュータに実行させるプログラム。

[13] 請求項12に記載のプログラムを記録したコンピュータ読み取り可能な記録媒体。

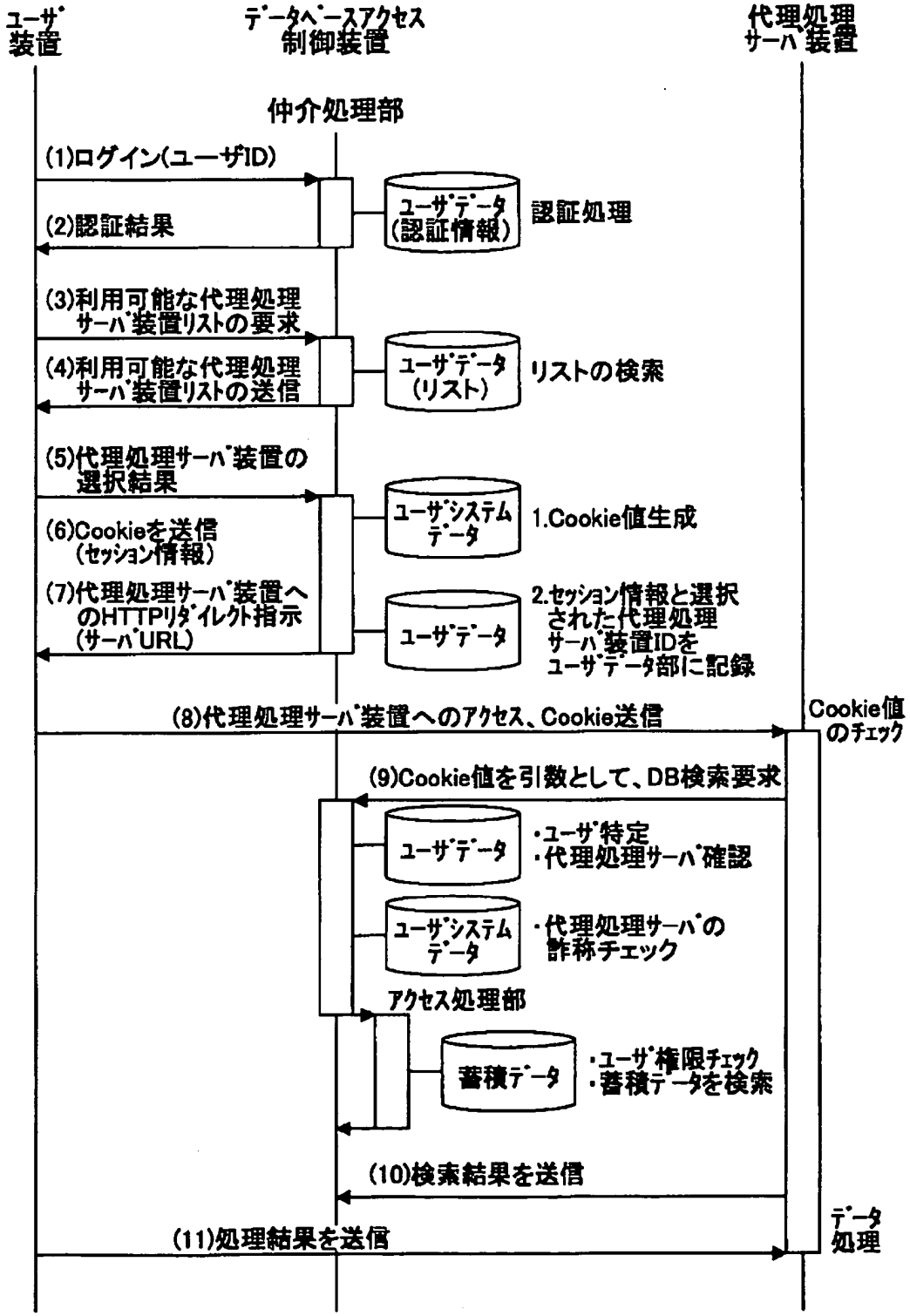
[図1]


データベース
200
100 データベースアクセス制御装置
アクセス処理部
102
仲介処理部
101
代理処理サーバ装置
300
代理処理サーバ装置
300
代理処理サーバ装置
300
ネットワーク
500
ユーザ装置
400
ユーザ装置
400
ユーザ装置
400
ユーザ装置
400

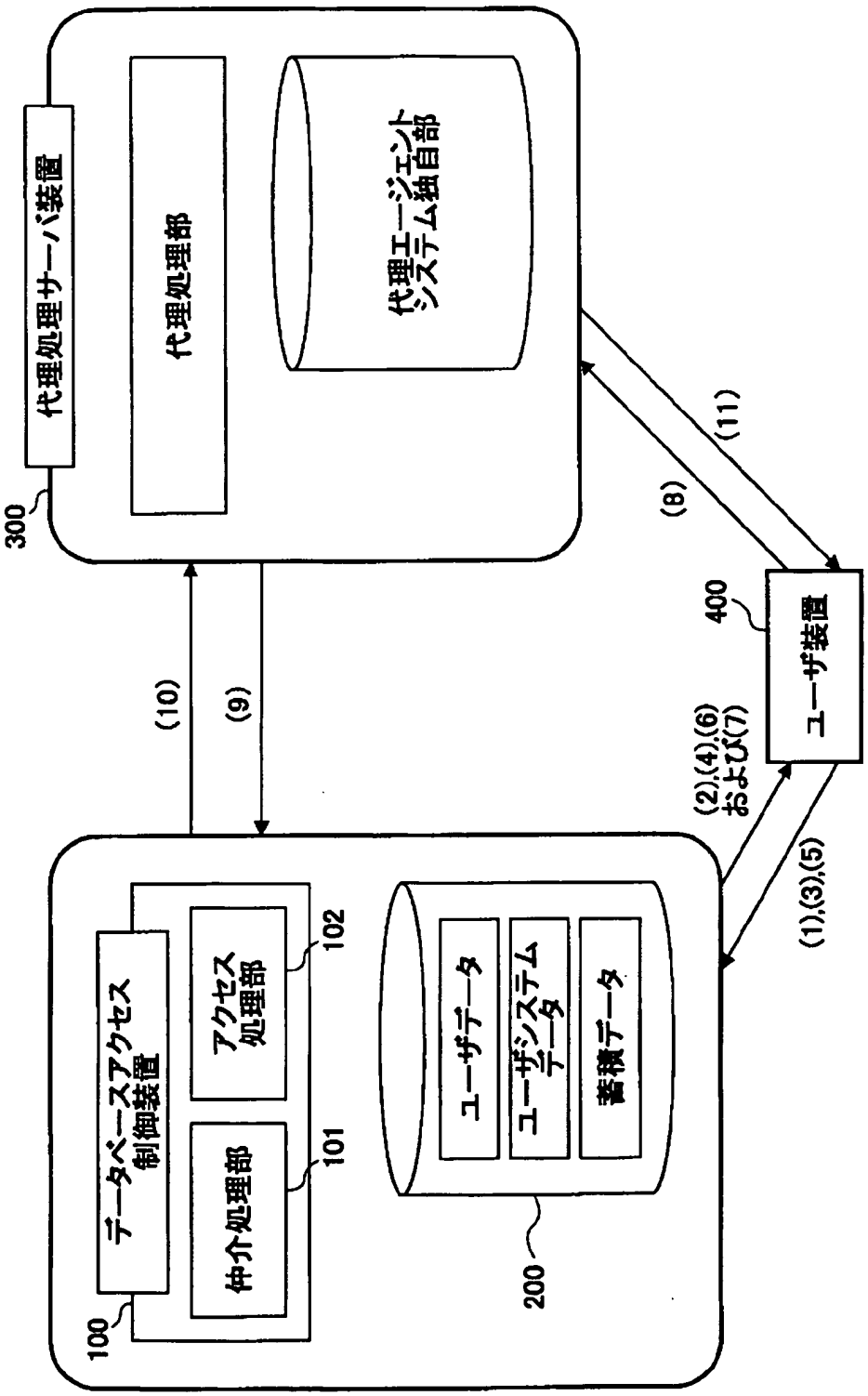
[図2]


データベース
210 ユーザデータ部
211 ユーザID
212 認証情報
213 ユーザ権限
214 セッション情報
215 代理処理サーバリスト
216 接続中の代理処理サーバID
220 ユーザシステムデータ部
221 代理処理サーバID
222 代理処理サーバURL
230 蓄積データ部
231 データ値
232 閲覧可能権限情報
100 データベースアクセス制御装置
仲介処理部
アクセス処理部
101
102

[図3]


ユーザ装置
データベースアクセス制御装置
代理処理サーバ装置
仲介処理部
(1)ログイン(ユーザID)
(2)認証結果
ユーザデータ(認証情報)
認証処理
(3)利用可能な代理処理サーバ装置リストの要求
(4)利用可能な代理処理サーバ装置リストの送信
ユーザデータ(リスト)
リストの検索
(5)代理処理サーバ装置の選択結果
(6)Cookieを送信(セッション情報)
(7)代理処理サーバ装置へのHTTPリダイレクト指示(サーバURL)
ユーザシステムデータ
1.Cookie値生成
ユーザデータ
2.セッション情報と選択された代理処理サーバ装置IDをユーザデータ部に記録
(8)代理処理サーバ装置へのアクセス、Cookie送信
Cookie値のチェック
(9)Cookie値を引数として、DB検索要求
ユーザデータ
・ユーザ特定
・代理処理サーバ確認
ユーザシステムデータ
・代理処理サーバの詐称チェック
アクセス処理部
蓄積データ
・ユーザ権限チェック
・蓄積データを検索
(10)検索結果を送信
(11)処理結果を送信
データ処理

[図4]


代理処理サーバ装置
代理処理部
代理エージェントシステム独自部
300
(11)
(8)
400
ユーザ装置
(10)
(9)
(2),(4),(6)および(7)
(1),(3),(5)
データベースアクセス制御装置
アクセス処理部
102
仲介処理部
101
100
ユーザデータ
ユーザシステムデータ
蓄積データ
200